# Software Assurance Program Working Groups

The DHS National Cyber Security Division (NCSD) has established working groups to support each of the Software Assurance Program's focus areas. Information about the working groups' activities is published on the Software Assurance Community Resources and Information Clearinghouse (CRIC), along with resources and information for a broad range of stakeholders.

For more information, please visit the CRIC[1]. For comments and inquiries, please email software.assurance [at] dhs.gov.

## Focusing Collaborative Efforts

Software Assurance Working Groups provide venues for public-private collaboration to focus on relevant portfolios of interest.

The Acquisition & Outsourcing[2] Working Group provides resources for incorporating software assurance considerations in key decisions for procurement and outsourcing within the acquisition life-cycle process.

The Processes & Practices[3] Working Group captures software assurance issues, shares sound practices and guidelines, and provides community input to national and international software assurance related standards and organizational benchmarking schemes.

The Workforce Education & Training[4] Working Group provides a common body of knowledge and model curriculum for education and training for improving skills and capabilities to produce secure software.

The Measurement[5] Working Group helps decision makers quantify and interpret security risk exposures by offering measures of software assurance and information security. The group facilitates the compatibility of network, system, and software testing, assessment, and monitoring tools output to integrate data sources for measurement.

The Technology, Tools & Product Evaluation[6] Working Group assists in advancing software assurance tools and technologies to improve the accuracy and coverage of evaluation and certification of software. It provides analysis of tools for evaluating exploitable weaknesses in software vulnerabilities and quality. It provides the framework for the Assurance Ecosystem and advances the evolution and use of common weakness enumerations for static code analyzers.

The Malware Working Group seeks tools and methods to categorize code behavior and defend against malicious software, enabling developers to design more resilient software.

The Business Case[7] Working Group advances the awareness and understanding of and the demand for assured software. It provides a venue for addressing the economics of software assurance.

[1] https://buildsecurityin.us-cert.gov/swa
[2] https://buildsecurityin.us-cert.gov/swa/acqwg.html
[3] https://buildsecurityin.us-cert.gov/swa/procwg.html
[4] https://buildsecurityin.us-cert.gov/swa/wetwg.html
[5] https://buildsecurityin.us-cert.gov/swa/measwg.html
[6] https://buildsecurityin.us-cert.gov/swa/TTPE_WG.html
[7] https://buildsecurityin.us-cert.gov/swa/bcwg.html